TRANSPERFECT

ALBANY
AMSTERDAM
ATLANTA
AUSTIN
BARCELONA
BERLIN
BOSTON
BRUSSELS
CHARLOTTE
CHICAGO
DALLAS
DENVER
DUBAI
DUBLIN
FRANKFURT
GENEVA
HONG KONG
HOUSTON
IRVINE
LONDON
LOS ANGELES
MIAMI
MINNEAPOLIS
MONTREAL
MUNICH
NEW YORK
ORLANDO
PARIS
PHILADELPHIA
PHOENIX
PORTLAND
RESEARCH TRIANGLE PARK
SAN DIEGO
SAN FRANCISCO
SAN JOSE
SEATTLE
SINGAPORE
STOCKHOLM
SYDNEY
TOKYO
TORONTO
VANCOUVER
WASHINGTON, DC

AFFIDAVIT OF ACCURACY

I, Anne Lutz, hereby certify that I am fluent in both English and French, and the following is, to the best of my knowledge and belief, a true and accurate translation of the following documents [Application No. 02 12 404] from French into English.

Anne Lutz
TransPerfect Translations
3 Park Ave
New York, NY 10016

Sworn to before me this
17th day of April, 2009

Signature, Notary Public

Katharine L Perekslis
Notary Public, State of New York
No. 01PE6181423
Qualified in QUEENS County
Commission Expires Jan 28 2012

Stamp, Notary Public

Washington, DC

The invention relates to a secure method of exchanging information messages sent successively, at given time intervals, from a transmitting platform to a receiving platform. More particularly, the invention concerns a method of ensuring that the last message received by the receiving platform corresponds to the last message sent by the transmitting platform.

The method according to the invention finds particular application in systems for the operation and/or supervision of trains, called SACEM (Système d'Aide à la Conduite, à l'Exploitation et à la Maintenance, or Driving, Operation and Maintenance Assistance System) comprising a centralized system control center, fixed installations along the tracks and control equipment in each train. In such driving systems, the centralized system control center transmits, at regular intervals of time, messages of information to the fixed installations, said messages comprising information related to the traffic conditions on one or more block sections located downstream from the fixed installation. The control equipment of any train located on the network then receives from the fixed installations the last message of information received by the fixed installation and deduces therefrom the operating speed to adopt. During the exchange of such messages of information it is essential, for reasons of safety, to be certain that the last message received by the fixed installations clearly corresponds to the last information message sent by the centralized system control center. However, because of the various components involved in transmitting messages and the relatively long distance that could exist between the centralized system control center and the fixed installations, some messages could be disrupted and delayed in their transmission and arrive late at the fixed installations, resulting in a change of the order of receipt of the information messages by the fixed installation compared to the order of transmission by the centralized system control center. In such a case the information updated at the fixed installation no longer corresponds to the last message actually sent by the centralized system control center. Although such phenomena are rare, they absolutely must be detected in order to ensure the safety of traffic.

Customarily, it is known that, in order to make the transmission of information messages secure, bidirectional and continuous exchanges of data are performed so that the information message received by the fixed installation is retransmitted to the centralized system control center which ensures its correspondence with the information message sent. However, such methods using bidirectional exchanges of data implement complex processing methods requiring expensive devices at the arrival and departure.

The purpose of the present invention is therefore to propose a secure method of exchanging information messages that makes it possible to ensure, during successive unidirectional exchanges of information messages between a transmitting platform and a receiving platform, that the last message received by the receiving platform clearly corresponds to the last message sent by the transmitting platform in order to be able to validate the correct updating of the information message at the receiving platform.

To that end, an object of the invention is a secure method of exchanging information messages sent successively from a transmitting platform to a receiving platform, characterized in that it comprises:

a) an initialization sequence in which at least one initialization message containing information relative to the sending date t_1 of the first information message M_1 is exchanged between the transmitting platform and the receiving platform so that both the transmitting and receiving platforms know the sending date t_1 of the first information message M_1.

b) a transmission sequence of information messages in which:

- the information messages are sent successively by the transmitting platform at time intervals ΔT_E given with a transmission time tolerance of δ ($\delta < \Delta T_E$), basing it on a clock pertaining to the transmitting platform, so that the first message M_1 is transmitted on the date t_1 of the clock and the n^{th} message Mn is sent on the date $t_n = t_1 + (n-1) * \Delta T_E + \delta$, each message M_n being coded with at least one dynamic code C_n pertaining to the sending date t_n of the message. Advantageously, the data

of the information messages are coded by a coding defined in accordance with the security criteria of the application, in order to make the information messages incomprehensible in the event of malfunction of the transmission. This coding, for example, is the SACEM coding.

- the messages received by the receiving platform are processed according to their reception date t_r, based on a clock pertaining to the receiving platform so that the messages received within an observation window F_n in the vicinity of t_n are decoded with a decoding sequence DC_n adapted for decoding the dynamic code C_n, the clock of the receiving platform being set at date t_1 upon receipt of the first message M_1.

According to particular embodiments, the method according to the invention can include one or more of the following characteristics taken individually or in any technically possible combination thereof:

- during the initialization sequence a), a coded initialization message M_0 is sent from the transmitting platform to the receiving platform, and a coded initialization message M'_0 is sent from the receiving platform to the transmitting platform, said initialization messages M_0, M'_0 containing the information related to the sending date $t_1$of the first information message M_1, said initialization messages M_0, M'_0 being decoded by the transmitting and receiving platforms which then know the sending date t_1 of the first information message M_1;

- in the event the first message M_1 is not received in the allowed time after the receipt of the initialization message, the clock of the transmitting platform is automatically set to the date t_1 at the moment corresponding to the end of the allowed time;

- the observation window F_n corresponds to a window of time $[t_1 + (n - 1)*\Delta T_E - \Delta T_{F*E}, t_1 + (n-1)*\Delta T_E + \Delta T_F * (1 - \varepsilon)]$, where n is a whole number and ΔT_F corresponds to the width of the observation window and has the relationship $\Delta T_F \leq \Delta TE$, and where ε falls between 0 and 1;

- a clock synchronization signal is transmitted regularly by the transmitting platform between the transmission of messages M_n, said synchronization signal being used to dynamically correct the frequency or phase of the internal clock of the receiving platform in order to reduce the phase or frequency deviation between the internal clocks of the receiving and transmitting platforms;

- the information messages decoded by the receiving platform are transmitted to a module for processing the information;

- the messages received by the receiving platform during an observation window F_n are stored sequentially in a memory that can store only one message at a time and in which only the message stored in this memory at the end of the observation window F_n is transmitted to the information processing module;

- the transmitting platform pertains to a centralized system control center of a supervision and management system for railroad traffic and the receiving platform pertains to a fixed installation located beside the railroad track and in which the information processing module is composed of control equipment placed on board a train traveling on a block section associated with the fixed installation.

The purposes, aspects and advantages of the present invention will be better understood from the following description of a particular embodiment, provided by way of non-limiting example, with reference to the appended drawings in which:

- figure 1 is a partial diagrammatical representation of a train supervision installation equipped with a secure method of exchanging information messages according to the invention;

- figure 2 is a flowchart representing the principal steps of the transmission method implemented by the transmitting platform in accordance with the secure exchange method according to the invention;

- figure 3 is a flowchart representing the principal steps of the processing method implemented by the receiving platform in accordance with the secure exchange method according to the invention.

- figure 4 illustrates on a time scale the transmission of initialization messages from a transmitting platform and the receiving of messages on a receiving platform and their processing in accordance with the secure exchange method according to the invention.

To facilitate the reading of the drawing, only those items necessary for the comprehension of the invention have been shown. The same items have been given the same reference numbers from one figure to another.

Figure 1 diagrammatically represents a centralized system control center 1 communicating information messages to fixed installations 2 placed beside a railroad block section, said messages comprising information relating to the traffic conditions on one or more block sections located downstream from the fixed installation 2. These messages are then sent in a known manner by a track circuit from the fixed installations 2 to a train 5, the train 5 including control equipment 6 using these information messages to determine how to proceed, such as the speed to adopt or the need to trigger an emergency stop.

To carry out the transmission of the information messages, the centralized system control center 1 comprises a transmitting platform 10 connected by transmission cables 4 to a receiving platform 20 located in the fixed installation 2. Each transmitting platform 10 and receiving platform 20 includes an internal clock.

The transmission sequence of information messages by the transmitting platform 10 in the secure exchange method according to the invention will now be described with reference to figure 2.

According to this figure, in a first step 101 of the secure exchange method, an initialization sequence is carried out in which a coded initialization message M_0 is transmitted from the transmitting platform 10 to the receiving platform 20. Said message

M_0 contains part of the information of the initial date of the first information message, generated by the transmitting platform, for example a random number. In a second step 102, the transmitting platform receives the message M'_0 which is transmitted by the receiving platform. Said message M'_0 contains part of the information of the initial date of the first information message, generated by the receiving platform, for example a random number. Said messages M_0, M'_0 are decoded in a step 103 by the transmitting platform 10 in order to generate the initial date of the first message. It is possible that a default part may complete this initial date.

The transmission security of the initialization sequence is customarily provided by a bidirectional exchange to ensure the proper correlation between the message received and the message sent.

The previously described initialization sequence is followed by a step 104 of the method in which no message is sent by the transmitting platform 10 until the time t_e of the internal clock of the transmitting platform 10 reaches the date t_1 prescribed for sending the first message M_1. At the date t_1, the transmitting platform 10 sends the first message M_1, messages then being sent at a constant interval of time ΔT_E so that the n^{th} message M_n is sent at the date $t_n = t_1 + (n - 1) * \Delta T_E + \delta$, n being a whole number, δ being the transmission time tolerance ($\delta < \Delta T_E$).

According to one characteristic of the invention, each message M_n sent is coded with a dynamic code C_n appropriate for the sending date t_n of the message. This dynamic code C_n is of the type selected from among the known dynamic codes that have coding properties such that the decoding of the message M_n with a decoding sequence other than the DC_n decoding sequence provided for decoding the code C_n results in obtaining an incomprehensible message due to the coding defined at the application. By way of example, the selected coding is an overlay of a pseudo-random sequence based on a primitive polynomial $X^{32} + X^{22} + X^2 + X + 1$ applied to each of the data bits.

The processing carried out in parallel by the receiving platform 20, during the sequence of transmission of the information messages by the transmitting platform 10, will now be described with reference to figure 3.

As shown in figure 3, in a first step 201 of the method the receiving platform 20 receives the message M_0 contained in the initialization sequence transmitted by the transmitting platform during the step 101. In a second step 202, the receiving platform 20 transmits the message M'_0 which is received by the transmitting platform during the step 102. In a step 203, these messages M_0, M'_0 are decoded by the receiving platform 20 in order to obtain the initial date t_1 of the first message M_1, as in the step 103 for the transmitting platform.

In a subsequent step 204 of the method, which step is triggered when the receiving platform 20 receives the first message M_1, the internal clock of the receiving platform 20 is set to the date t_1 so that $t_r = t_1$ at the moment of receipt of this first message M_1, where t_r is the time on the internal clock of the receiving platform 20. The internal clock of the receiving platform 20 is also set by default to the date t_1 if the first message M_1 does not arrive at the receiving platform 20 within the time allowed after receipt of the initialization message M_0.

Preferably, after the receipt of the message t_1, the clock of the receiving platform 20 is regularly synchronized to the clock of the transmitting platform 10 from clock synchronization frames regularly transmitted by the transmitting platform 10 in the same cycle as the messages M_n. These frames are either specific or are themselves composed of messages M_n. Thus, when a synchronization deviation (phase, frequency, average, least squares, etc.) is measured between the internal clock of the transmitting platform 10 and the internal clock of the receiving platform 20, a correction of the frequency or phase of the internal clock of the receiving platform 10 is performed dynamically so as to reduce the phase or frequency deviation between the two clocks.

During the next step 205 of the method, the first received message M_1 is decoded by means of a decoding sequence DC_1 adapted for decoding the dynamic code C_1 and the result of the decoded message M_1 is transmitted by the receiving platform 20 to the track circuit.

The next step 206 of the method is triggered iteratively when the receiving platform 20 receives a new message $M_?$, in principle the message M_n, at a moment t_r that falls within the time observation window F_n, [which] corresponds to a window of time $[t_1 + (n - 1) * \Delta T_E - \Delta T_F * \varepsilon, t_1 + (n - 1) * \Delta T_E + \Delta T_F * (1 - \varepsilon)]$, where ΔT_F is the width of the observation window, n is a whole number and ε falls between 0 and 1.

During the next step 207 of the method, the message $M_?$ received within an observation window F_n of the transmitting platform 20 [*sic*] is decoded by means of a decoding sequence DC_n assigned to this observation window F_n and corresponding to the inverse coding sequence DC_n adapted for decoding only the dynamic code C_n of the n^{th} message transmitted by the transmitting platform 10.

In one preferred embodiment of the invention, the message $M_?$ decoded by the receiving platform 20, in a step not shown in figure 3 is then stored temporarily in a memory having a capacity permitting the storage of only one message at a time, before being sent to the track circuit at the moment t_r corresponding with the end of the observation window F_n. In a simplified variation, the message $M_?$ can also be transmitted to the track circuit as soon as the end of step 207 is reached, without being stored in a memory.

When the train 5 is on the block section, it receives by means of the track circuit the messages decoded by the receiving platform 20, with the assurance that the messages $M_?$ received, which have become comprehensible as the result of the decoding defined at the application, are correctly updated messages M_n whose information should be taken into account. Moreover, to ensure the security of train traffic on the track, it is provided that the control equipment 6 on board the train 5 trigger an emergency stop when the train 5 successively receives a plurality of incomprehensible messages, for example five messages in a row, so that the train is stopped when there is no longer enough information about the traffic conditions on the block section downstream.

Figure 4 illustrates, by way of example, an exchange sequence of information message according to the method of the invention. In this figure, the transmission of messages M_1 to M_6 is represented on the upper axis t_e, this axis corresponding to the elapsed time on the internal clock of the transmitting platform 10, and the receipt of messages is represented on the axis t_r corresponding to the elapsed time on the clock of the receiving platform 20. For the example described in figure 4, the initialization sequence, not shown in the figure, will be considered to be initiated at the moment t_e = 4:59 a.m. and the date t_1 of sending the first message is t_1 = 5 a.m. The interval ΔT_E is on the order of a few milliseconds, e.g., ΔT_E = 50 ms, so that the updating of the information messages is regular. In the example shown, the transmission time tolerance δ is zero and the observation windows F_n have the characteristics $\varepsilon = 0.5$ and $\Delta T_F = 25$ ms.

Thus, with reference to figure 4 and particularly to the receipt of messages on the lower axis t_r representing the elapsed time on the clock of the receiving platform 20, several moments after the transmission of the message M_1 the receiving platform 20 receives the first message M_1. The receiving platform 20 then proceeds to set its internal clock so that $t_r = t_1$ at the moment of receipt of the message M_1. The message M_1 is then decoded by the receiving platform by means of the decoding sequence DC_1, then transmitted to the track circuit and therefore to any train 5 that may be present on the block section.

Several moments later, the receiving platform 20 receives the message M_2 in the observation window F_2, which is centered on t_2 and has a width ΔT_F. The receiving platform 20 then proceeds to decode the message M_2 with the decoding sequence DC_2. This decoded message is stored in a memory of the receiving platform that has a capacity allowing only one message at a time to be stored, and is then transmitted to the track circuit at the moment t_r corresponding to the end of the observation window F_2, or $t_r = t_2 + \Delta T_F / 2$. The control equipment 6 of the train 5 on the block section then receives information about the traffic conditions by the message M_2.

During the observation window F_3, no message is received by the receiving platform 20, following disturbances in the transmission of the message M_3. In this case, the message

transmitted by the receiving platform 20 to the track circuit at the moment t_r, corresponding to the end of the observation window F_3, is incomprehensible due to the coding of the application, so that the control equipment 6 of the train 5 on the block section is notified of this fault in the updating of the information messages.

When the message M_3 has finally been received in the observation window F_4, said message M_3 is then decoded with the decoding sequence DC_4 assigned to the window F_4 which results in obtaining a decoded message that is incomprehensible thanks to the coding of the application which is stored in the memory of the receiving platform 20. This incomprehensible message is transmitted to the track circuit at the moment t_r corresponding to the end of the observation window F_4 and the control equipment 6 of the train 5 receives this incomprehensible message which it interprets as a new fault in the updating of the information messages. The control equipment 6 then counts two successive faults in updating the information messages but does not yet cause an emergency stop of the train if the permitted tolerance is five successive faults.

During the observation window F_5, two messages M_4 and M_5 are received successively by the receiving platform 20. Initially the receiving platform 20 receives the message M_4 then the message M_5 in the same observation window F_5. The receiving platform proceeds to decode this last message M_5 by the decoding sequence DC_5, resulting in obtaining a decoded message that is again comprehensible due to the coding of the application, which is stored in the memory of the receiving platform 20 instead of the preceding message. This message M_5 is transmitted to the track circuit at the moment t_r corresponding to the end of the observation window F_5. The control equipment 6 of the train 5 then receives a message, the message M_5, that is comprehensible thanks to the coding of the application, and there thus is assurance that the information contained in said message is correctly updated information.

During the observation window F_6, the receiving platform 20 receives the message M_6 which is decoded by the decoding sequence DC_6, then stored in the memory before being

sent to the circuit at the moment t_r corresponding to the end of the window F_6. The control equipment 6 of the train 5 then receives a message, the message M_6, that is comprehensible thanks to the coding of the application and there is thus assurance that the information contained in this message is updated information.

Thus, such a transmission method for the secure exchange of information messages makes it possible, by a regular unidirectional exchange of messages between a transmitting platform and a receiving platform, to ensure the proper updating of information messages that arrive comprehensibly at the recipient, and does so without the use of complex processing means. Such a method has the advantages of being inexpensive to implement and of allowing the high speed transmission of information, unlike customary bidirectional transmission systems in which the information verification sequence considerably slows down the transmission of messages and thus their recognition. The method according to the invention thus makes it possible to have a high refresh rate of messages received by the train.

Obviously, the invention is in no way limited to the embodiment described and illustrated, which has been provided solely by way of example. Modifications remain possible, particularly from the point of view of the composition of the various elements or by substitution of technical equivalents, without going beyond the domain of protection of the invention.

CLAIMS

1) Secure method of exchanging information messages sent successively from a transmitting platform (10) to a receiving platform (20), characterized in that it comprises:

a) an initialization sequence in which at least one initialization message containing information relative to the sending date t_I of the first information message M_I is exchanged between the transmitting platform (10) and the receiving platform (20) so that both the transmitting (10) and receiving (20) platforms know the sending date t_I of the first information message M_I.

b) a transmission sequence of information messages in which:

- the information messages are sent successively by the transmitting platform (10) at time intervals ΔT_E given with a transmission time tolerance of δ, basing it on a clock pertaining to the transmitting platform (10), so that the first message M_I is transmitted on the date t_I of the clock and the n^{th} message M_n is sent on the date $t_n = t_I + (n-1) * \Delta T_E + \delta$, each message M_n being coded with at least one dynamic code C_n pertaining to the sending date t_n of the message.

- the messages received by the receiving platform (20) are processed according to their reception date t_r, based on a clock pertaining to the receiving platform (20) so that the messages received within an observation window F_n in the vicinity of t_n are decoded with a decoding sequence DC_n adapted for decoding the dynamic code C_n, the clock of the receiving platform (20) being set at date t_I upon receipt of the first message M_1.

2) Secure method of exchanging information messages as claimed in claim 1, characterized in that during the initialization sequence a), a coded initialization message M_0 is sent from the transmitting platform (10) to the receiving platform (20), and a coded initialization message M'_0 is sent from the receiving platform (20) to the transmitting platform

(10), said initialization messages M_0, M'_0 containing the information related to the sending date $t_1$of the first information message M_1, said initialization messages M_0, M'_0 being decoded by the transmitting (10) and receiving (20) platforms which then know the sending date t_1 of the first information message M_1.

3) Secure method of exchanging information messages as claimed in either of claims 1 or 2, characterized in that in the event the first message M_1 is not received in the allowed time after the receipt of the initialization message, the clock of the transmitting platform (20) [*sic*] is automatically set to the date t_1 at the moment corresponding to the end of the allowed time

4) Secure method of exchanging information messages as claimed in any one of claims 1 to 3, characterized in that the observation window F_n corresponds to a window of time $[t_1 + (n - 1) * \Delta T_E - \Delta T_F * \varepsilon, t_1 + (n-1) * \Delta T_E + \Delta T_F*(1 - \varepsilon)]$, where ΔT_F corresponds to the width of the observation window and has the relationship $\Delta T_F \leq \Delta TE$, and where ε falls between 0 and 1.

5) Secure method of exchanging information messages as claimed in any one of claims 1 to 4, characterized in that a clock synchronization signal is transmitted regularly by the transmitting platform (10) between the transmission of messages M_n, said synchronization signal being used to dynamically correct the frequency or phase of the internal clock of the receiving platform (20) in order to reduce the phase or frequency deviation between the internal clocks of the receiving (20) and transmitting (10) platforms.

6) Secure method of exchanging information messages as claimed in any one of claims 1 to 5, characterized in that the information messages decoded by the receiving platform (20) are transmitted to a module for processing the information (6).

7) Secure method of exchanging information messages as claimed in any one of claims 1 to 6, characterized in that the messages received by the receiving platform (20) during an observation window F_n are stored

sequentially in a memory that can store only one message at a time and in which only the message stored in this memory at the end of the observation window F_n is transmitted to the information processing module (6).

8) Secure method of exchanging information messages as claimed in any one of claims 1 to 7, characterized in that the transmitting platform (10) pertains to a centralized system control center (1) of a supervision and management system for railroad traffic and the receiving platform (20) pertains to a fixed installation (2) located beside the railroad track and in which the information processing module (6) is composed of control equipment (5) placed on board a train traveling on a block section associated with the fixed installation (2).

1 / 3

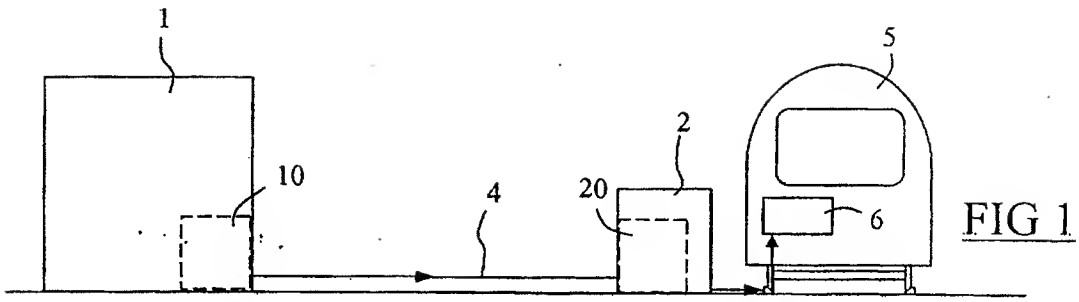

1
10
4
20
2
5
6

FIG 1

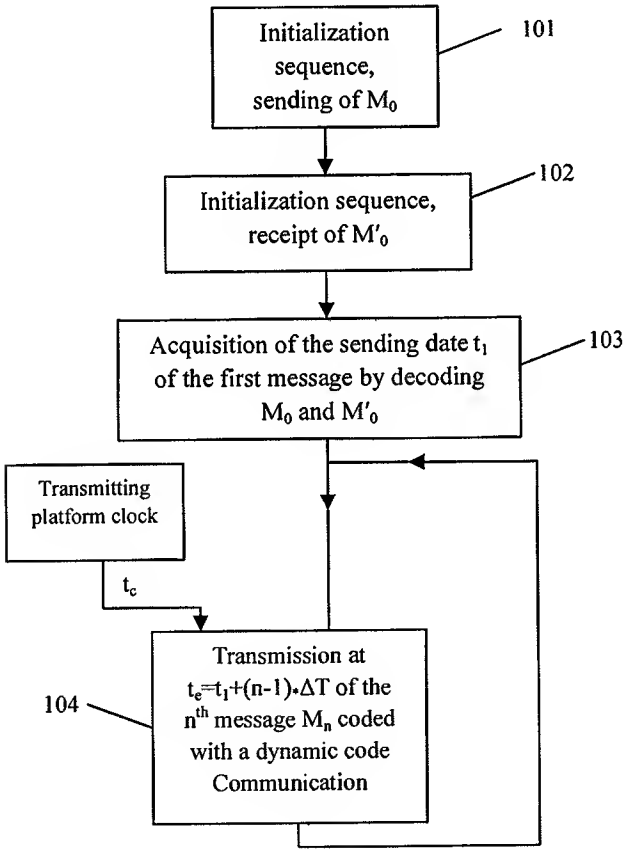

Initialization sequence, sending of M_0
101
Initialization sequence, receipt of M'_0
102
Acquisition of the sending date t_1 of the first message by decoding M_0 and M'_0
103
Transmitting platform clock
t_c
Transmission at $t_e=t_1+(n-1)\cdot\Delta T$ of the n^{th} message M_n coded with a dynamic code Communication
104

FIG 2

2 / 3

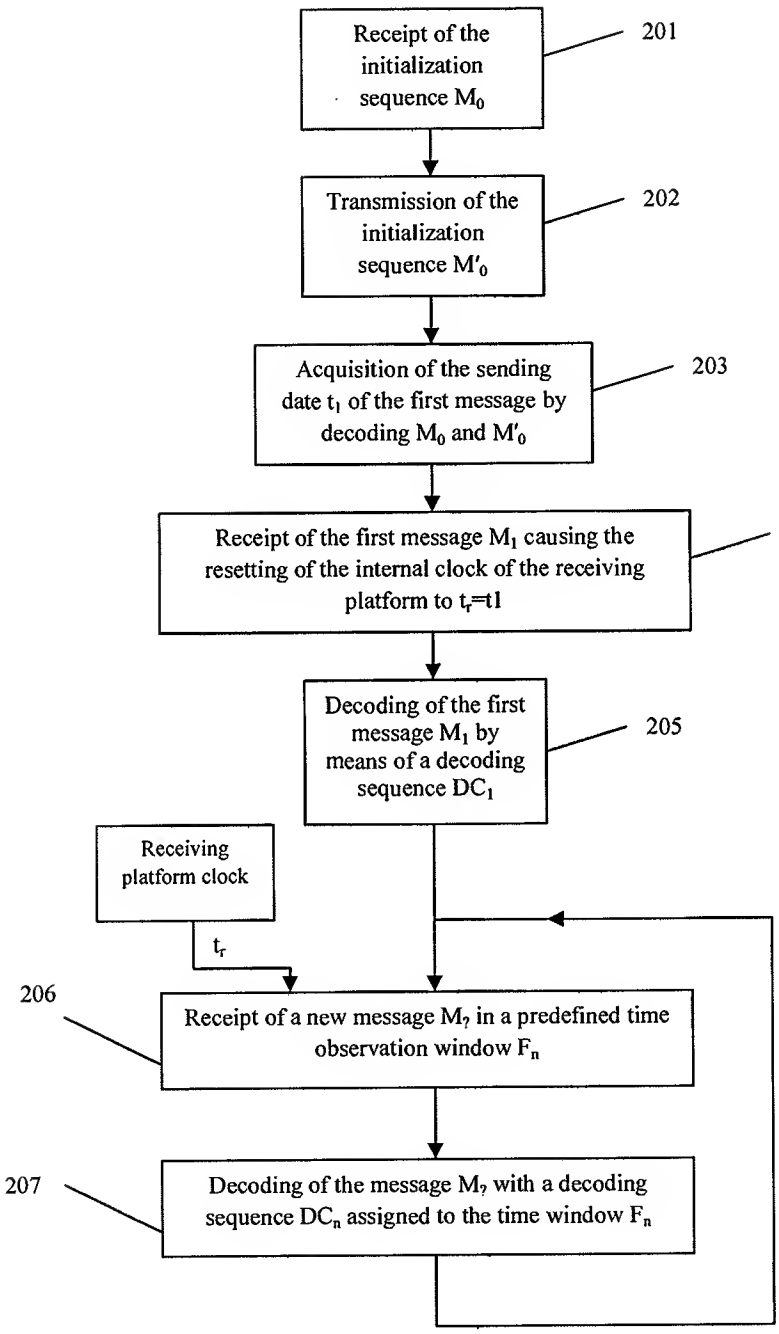
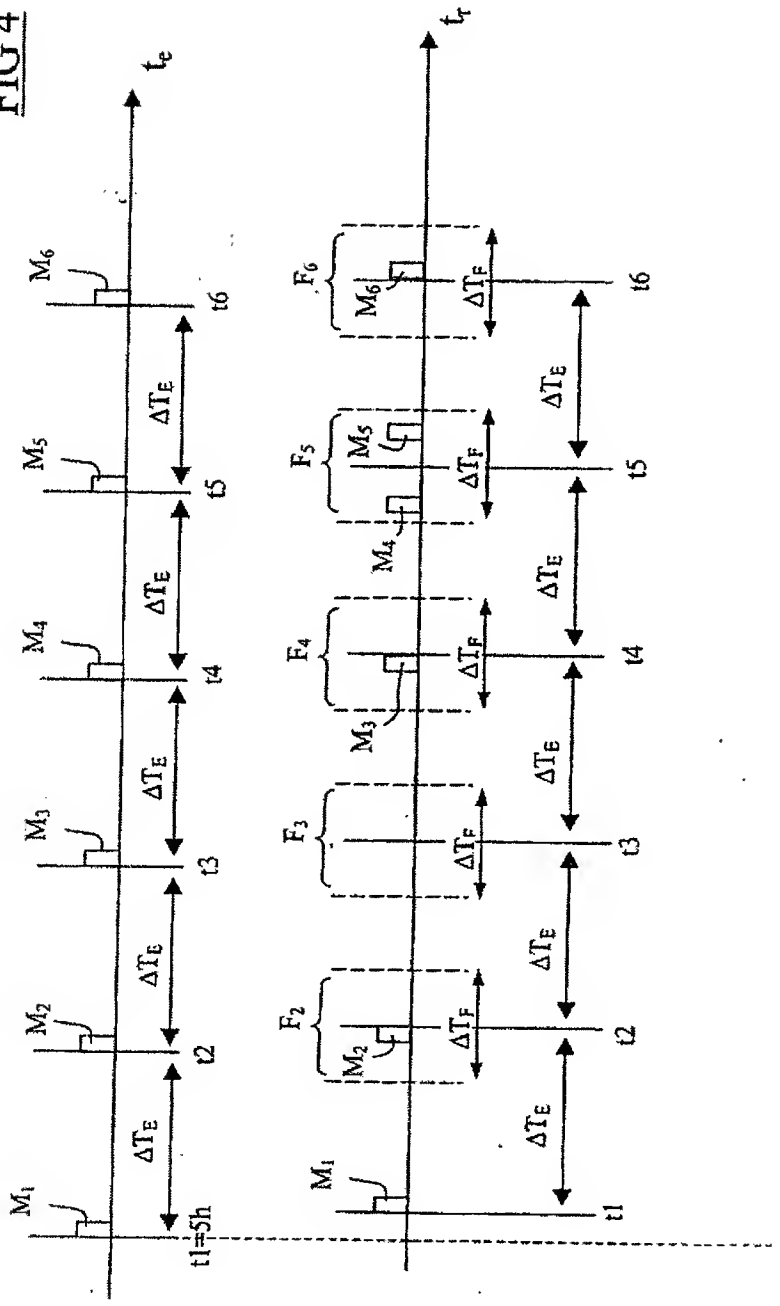

Receipt of the initialization sequence M_0
201
Transmission of the initialization sequence M'_0
202
Acquisition of the sending date t_1 of the first message by decoding M_0 and M'_0
203
Receipt of the first message M_1 causing the resetting of the internal clock of the receiving platform to t_r=t1
204
Decoding of the first message M_1 by means of a decoding sequence DC_1
205
Receiving platform clock
t_r
206
Receipt of a new message $M_?$ in a predefined time observation window F_n
207
Decoding of the message $M_?$ with a decoding sequence DC_n assigned to the time window F_n

FIG 3

3 / 3

FIG 4


t_e
t_r
M_1
M_2
M_3
M_4
M_5
M_6
F_2
F_3
F_4
F_5
F_6
ΔT_E
ΔT_F
t1=5h
t1
t2
t3
t4
t5
t6